JOURNAL OF ALGEBRA 99, 430–437 (1986)

Invariants of Finite Cyclic Groups Acting on Generic Matrices

JOE W. FISHER

University of Cincinnati, Cincinnati, Ohio 45221

AND

S. MONTGOMERY*

University of Southern California, Los Angeles, California 90089

Communicated by I. N. Herstein

Received June 27, 1984

INTRODUCTION

A classical theorem of E. Noether asserts that if R is a commutative ring, finitely generated over a field k, and G is any finite group of k-automorphisms of R, then the fixed ring (or ring of invariants) R^G is also finitely generated. The question naturally arises as to what extent Noether's theorem can be generalized to the noncommutative case. If R is also Noetherian and $|G|^{-1} \in k$, all is well: R^G is finitely generated, a result of Montgomery and Small [6]. However, it is false in general, even for *PI* rings [6]. Moreover, a recent result in Dicks and Formanek [1] (and, somewhat later, Kharchenko [4]), shows that almost the opposite of Noether's theorem holds in the free algebra. That is, they prove that if G acts linearly on the free algebra $F = k\langle x_1,..., x_d\rangle$, then F^G is finitely generated if and only if G acts by scalar matrices.

In the present paper we consider the analogous problem for an algebra of generic matrices. That is, let $U = k\{X_1,..., X_d\}$ be the generic matrix algebra generated over a field k by the $m \times m$ $(m \geqslant 2)$ generic matrices $X_1,..., X_d$ $(d \geqslant 2)$. Let G act linearly on U; that is, for each $g \in G$, $X_i^g = \sum_j \alpha_{ij} X_j$, for $\alpha_{ij} \in k$. Thus g corresponds to the dxd matrix $A = (\alpha_{ij})$.

If G consists of scalar matrices and $|G|^{-1} \in k$, then U^G is always finitely generated. For, consider the free algebra $F = k\langle x_1,..., x_d\rangle$ with the same action; since $U = \bar{F}$, a homomorphic image of F, it follows that $U^G =$

* Research of the second author was partially supported by NSF Grant MCS-83-01393.

0021-8693/86 $3.00

$\bar{F}^G = \overline{F^G}$ (since $|G|^{-1} \in k$), and thus U^G is finitely generated since F^G is finitely generated. However, the converse of this is false, as is shown by an example of Montgomery and Passman [5] of a nonscalar automorphism of order 3 of 2×2 generic matrices such that U^G is still finitely generated. Thus, the analog of Dick's and Formanek's theorem does not hold.

However, the main result of this paper shows, at least for cyclic groups, that for matrices which are large enough compared to $|G|$, the generic matrices behave like the free algebra. We prove:

THEOREM 3: *Let $G = \langle g \rangle$ be a cyclic group of order n acting linearly on $U = k\{X_1,..., X_d\}$, the generic matrix algebra of mxm matrices over the field k, where $d, m \geqslant 2$, and let A be the matrix corresponding to g. Assume that n is a unit in k and that A is not scalar. Then U^G is not finitely-generated whenever $m \geqslant n - [\sqrt{n}] + 1$.*

Moreover, if A has a characteristic root α such that $\alpha^q = 1$, some q with $0 < q < n$, then U^G is not finitely-generated whenever $m \geqslant 2$.

The proof divides into two separate arguments, as to whether or not all the characteristic roots of A have (multiplicative) order n.

1. Characteristic Roots of Different Orders

We begin with the following proposition.

PROPOSITION 1. *Let l and N be positive integers and let $p(x, y) \in k\langle x, y\rangle$ be a nonzero homogeneous polynomial of x-degree $l+1$ and y-degree N of the form $p(x, y) = x^l y^N x + y q_1(x, y) + q_2(x, y)\, y$ for some $q_i \in k\langle x, y\rangle$. Then $p(x, y)$ is not an identity for mxm matrices for any $m \geqslant 2$.*

Proof. We will show that if $A = \begin{pmatrix} 0 & 1 \\ 1 & z \end{pmatrix}$, for z an indeterminate over k, and $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, the specialization $x \to A$ and $y \to B$ gives $p(A, B) \neq 0$. In particular, we show that the (2, 2) entry of $p(A, B)$ is a monic polynomial in z of degree $l-1$.

First, note that for any 2×2 matrices C and D, the matrix $BC + DB$ has 0 as its (2, 2) entry. Thus the $yq_1 + q_2 y$ terms contribute nothing, and we only must consider $x^l y^N x$.

Write $A^l = (a_{ij,l})$. Then $A^l B^N A = \begin{pmatrix} 0 & a_{11,l} \\ 0 & a_{21,l} \end{pmatrix}$, so it will suffice to show that $a_{21,l}$ is a monic polynomial in z of degree $l-1$. One can see this by induction, as follows:

As we find each successive power of A, the entries "move" in the following way: $(\uparrow \leftrightarrows \uparrow)$. That is, for any $l \geqslant 2$,

$$a_{21,l+1} = a_{12,l+1} = a_{22,l}, \quad a_{11,l+2} = a_{22,l}, \quad \text{and} \quad a_{11,l+1} = a_{22,l-1}.$$

Moreover, $a_{22,l+1} = za_{22,l} + a_{12,l}$, which is a monic polynomial in z of degree $l+1$, by induction on l. Thus $a_{21,l} = a_{22,l-1}$, a polynomial of degree $l-1$. The proposition is proved.

LEMMA 1. *In the free algebra $k\langle x, y\rangle$, define $g \in \operatorname{Aut} k\langle x, y\rangle$ by $x \to \omega x$ and $y \to \gamma y$ where ω and γ are* n*th roots of unity with orders a and b, respectively $(a > b)$. If a_1 is the order of ω* mod$\langle\gamma\rangle$, *then any monomial $m(x, y)$ which is fixed by g and has x-degree at least one must have x-degree at least a_1.*

Proof. Suppose that $m(x, y)$ has x-degree $r \geqslant 1$ and y-degree s. Then $m(x, y)^g = \omega^r \gamma^s m(x, y) = m(x, y)$. Hence $\omega^r = \gamma^{-s} \in \langle\gamma\rangle$. Thence $a_1 \mid r$ and so $r \geqslant a_1$.

Since a_1 is the order of ω mod$\langle\gamma\rangle$, there is a t $(0 \leqslant t < b)$ such that $\omega^{a_1} = \gamma^t$.

COROLLARY 1. *Let g be as in Lemma* 1 *and choose $N > t$. Then*

(i) *$x^{a_1-1}y^{bN-t}x$ is fixed by g and has no initial segments fixed by g.*

(ii) *any monomial of x-degree a_1 and y-degree $bN-t$ which is a product of at least two other monomials fixed by g must either begin with y or end with y.*

Proof. (i) Write $m(x, y) = x^{a_1-1}y^{bN-t}x$. Then $m(x, y)^g = \omega^{a_1}\gamma^{bN-t}m(x, y)$. Then $\omega^{a_1}\gamma^{bN-t} = \gamma^t\gamma^{-t} = 1$. Thus $m(x, y)$ is fixed; however, Lemma 1 guarantees that $m(x, y)$ has no initial segments which are fixed by g.

For (ii), Lemma 1 implies that at most one fixed monomial factor can contain any power of x. The other monomial factors must therefore all be powers of y.

THEOREM 1. *Let $U = k\{X, Y\}$ where X and Y are mxm $(m \geqslant 2)$ generic matrices. Suppose that* $\operatorname{Aut}_k(U)$ *is given by $X^g = \omega X$ and $Y^g = \gamma Y$ where ω and γ are* n*th roots of unity. If ω and γ have distinct orders, then $U^{\langle g\rangle}$ is not finitely generated.*

Proof. We may assume that $o(\omega) = a > b = o(\gamma)$. Now if $U^{\langle g\rangle}$ is finitely generated we may assume that the generators $\{G_1, \ldots, G_s\}$ are images of monomials $\{g_1, \ldots, g_s\}$ in the free algebra which are fixed by the same action. Let N be the maximal degree of any $\{g_i\}$; assume also that $N > t$. With the notation as in Corollary 1, $X^{a_1-1}Y^{bN-t}X$ in $U^{\langle g\rangle}$ must be expressed as a polynomial in the $\{G_i\}$, $X^{a_1-1}Y^{bN-t}X = q(G_1, \ldots, G_s)$. Equivalently, $x^{a_1-1}y^{bN-t}x - q(g_1, \ldots, g_s)$ is an identity of mxm matrices. By the homogeneity of the T-ideal, q may be replaced by a sum of monomials, all of which have x-degree a_1 and y-degree $bN-t$. By the corollary $q=yq_1+q_2y$. But then $x^{a_1-1}y^{bN-t}x+yq_1+q_2y$ is an identity for mxm matrices, a contradiction.

2. Characteristic Roots of the Same Orders

We require the following fact about polynomial identities.

Proposition 2. *Let n, p, and N be positive integers with $1 \leqslant p < n$, and let $p(x, y) \in k\langle x, y\rangle$ be a nonzero homogeneous polynomial of y-degree N and x-degree $pN+n$. Assume that $p(x, y)$ contains exactly one monomial of the form*

$$m_0(x, y) = x^q(yx^p)^N x^{n-q}$$

with $p+1 \leqslant q \leqslant n-1$. Then $p(x, y)$ is not an identity for mxm matrices for any $m \geqslant p+2$.

We will prove the proposition by means of specialization $x \to A$, $y \to B$ such that $p(A, B) \neq 0$, where A and B are the following $(p+2) \times (p+2)$ matrices:

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & z \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & \\ \cdot & \\ 0 & \bigcirc \\ 1 & \\ 0 & \end{pmatrix} = E_{p+1,1},$$

where z is an indeterminate over the field k.

Lemma 2. *Write $A^k = (a_{ij,k})$ for $k \geqslant 0$. Then A and B have properties:*

(1) *$BA^kB = a_{1,p+1,k}B$ for all k.*

(2) *$a_{1,p+1,k} = 0$ for $k = 0, 1, \ldots, p-1$ and for $k = p+1, \ldots, 2p+1$; $a_{1,p+1,p} = 1 = a_{1,p+1,2p+2}$, and for all $k \geqslant 2p+2$, $a_{1,p+1,k}$ is a polynomial in z of degree $k-(2p+2)$.*

(3) *if $c(k, l)$ denotes the $(p+2, p+2)$ entry of A^kBA^l, for $k, l \geqslant 0$, then $c(k, l) = 0$ if either $k \leqslant p$ or $l \leqslant p$; if both $k, l \geqslant p+1$, then $c(k, l)$ is a polynomial in z of degree $k+l-(2p+2)$.*

Proof. The powers of A may be obtained inductively as follows: if A^k has columns $(C_1, C_2, \ldots, C_{p+2})$, then A^{k+1} has columns $(C_{p+2}, C_1, C_2, \ldots, C_p, D)$; similarly if A^k has rows $(R_1, R_2, \ldots, R_{p+2})^{\mathrm{T}}$, then A^{k+1} has rows $(R_2, \ldots, R_{p+2}, S)^{\mathrm{T}}$. Thus the only new entry to be computed is the

481/99/2-11

$(p+2, p+2)$ entry, which is easily seen to be a polynomial in z of degree $k+1$ (since $a_{p+2,p+2,k}$ is a polynomial of degree k).

(1) For any matrix $W=(w_{ij})$, it is clear that $BWB=w_{1,p+1}B$. Hence (1) follows.

(2) It is evident from the above that $a_{1,p+1,k}=0$ for $k=0,\ldots,p-1$ and for $k=p+1,\ldots,2p+1$, and that $a_{1,p+1,p}=1$. The rest of (2) follows from the fact that it takes $2p+2$ "moves" for the $(p+2, p+2)$ entry of A^0 to get to the $(1, p+1)$ position ($p+1$ column moves to the $(p+2, p+1)$ position followed by $p+1$ row moves up to the $(1, p+1)$ position).

(3) First, check that the $(p+2, p+2)$ entry of A^kBA^l is $a_{p+2,p+1,k}$ $a_{1,p+2,l}$. For any l, we claim that $a_{1,p+2,l}=a_{1,p+1,l+(p+1)}=a_{p+2,p+1,l}$. The first equality follows by moving the $(1, p+2)$ entry horizontally with $p+1$ moves. The second equality follows by moving the $(p+2, p+1)$ entry up the $p+1$ column. Thus the $(p+2, p+2)$ entry of A^kBA^l is $c(k, l)=a_{1,p+1,k+p+1}a_{1,p+1,l+p+1}$. Using (2), it is clear that if $k \leqslant p$ or $l \leqslant p$, then $c(k, l)=0$. If both k and l are equal to or greater than $p+1$, then again by (2), $c(k, l)$ is a polynomial of degree $k+p+1-(2p+2)+l+p+1-(2p+2) = k+l-(2p+2)$. The lemma is proved.

Proof of Proposition 2. Since we wish to show that $p(A, B) \neq 0$, we may ignore any monomials which go to zero. Since $BA^kB=0$ for $k=0, 1,\ldots, p-1$ and for $k=p+1,\ldots, 2p+1$, we need only consider monomials in $p(x, y)$ of the form

$$m(x, y)=x^{i_0}yx^{i_1}y\cdots yx^{i_{N-1}}yx^{i_N},$$

where $\sum_{j=0}^N i_j=pN+n$, and for $j=1, 2,\ldots, N-1$, either $i_j=0$, or $i_j=p$, or $i_j \geqslant 2p+2$. We consider the $(p+2, p+2)$ entry in all such $m(A, B)$. Now let r be the number of i_j, $1 \leqslant j \leqslant N-1$, which have degree $\geqslant 2p+2$. By renumbering, we may assume that $i_1, i_2,\ldots, i_r \geqslant 2p+2$ and $i_{r+i}=\cdots=i_{N-1}=p$. Then

$$m(A, B)=A^{i_0}BA^{i_1}B\cdots BA^{i_{N-1}}BA^{i_N}=\left(\prod_{j=1}^r a_{1,p+1,i_j}\right)A^{i_0}BA^{i_N}$$

by Lemma 2, part (1). Since we are interested in the $(p+2, p+2)$ entry, we may throw away any monomials with $i_0 \leqslant p$ or $i_N \leqslant p$ by Lemma 2, part (3). For i_0, $i_N \geqslant p+1$, Lemma 2 gives that $m(A, B)$ has $(p+2, p+2)$ entry of z-degree

$$d=\sum_{j=1}^r [i_j-(2p+2)]+i_0+i_N-(2p+2).$$

By using that $\sum_{j=r+1}^{N-1} (i_j-p)=0$ and $\sum_{j=0}^N i_j=pN+n$, we have that $d=n-(p+2)(r+1)$.

The *only* monomial with $r=0$ and a nonzero $(p+2, p+2)$ entry is $m_0(x, y)$; for $r=0$ gives that all $i_j=p$ for $j=1,..., N-1$, and so $i_0+i_N=p+n$. However, both i_0 and i_N are greater than or equal $p+1$. Hence $i_0 \leqslant p+n-(p+1)=n-1$. By assumption $m_0(x, y)$ is the only monomial with this property, and its $(p+2, p+2)$ entry has degree $d=n-(p+2)$, which is larger than the degree of any other $(p+2, p+2)$ entry. This is a contradiction. Whence, the proposition is proved.

THEOREM 2. *Let $U=k\{X, Y\}$ where X and Y are mxm $(m \geqslant 2)$ generic matrices. If δ is a primitive* n*th root of unity and g in $\mathrm{Aut}_k(U)$ is given by $X^g=\delta X$ and $Y^g=\delta^t Y$ with $1<t \leqslant n$, then $U^{\langle g \rangle}$ is not finitely generated whenever $m \geqslant n-t+2$.*

Proof. In Proposition 2 let $p=n-t$. When $p=0$ (so $\delta^t=1$), Theorem 1 shows that $U^{\langle g \rangle}$ is not finitely generated for $m \geqslant 2=n-t+2$. Thus we may assume that $p \geqslant 1$.

Assume to the contrary that $U^{\langle g \rangle}$ is finitely generated by, say, $\{G_1,..., G_s\}$ where each G_i is the image of a homogeneous invariant element g_i in the free algebra $k\langle x, y\rangle$, and deg $(g_i) \leqslant N$ for all $i=1, 2,..., s$. Now in the free algebra, it is easy to see that for all q, $p+1 \leqslant q \leqslant n-1$, the fixed monomials

$$x^q(yx^p)^N x^{n-q} \qquad (*)$$

have no initial segments fixed by g, and so cannot be a product of invariants in $k\langle x, y\rangle$ of lower degree. We choose one of these monomials, say $m_0(x, y)=x^{n-1}(yx^p)^N x$.

In $U^{\langle g \rangle}$, $m_0(X, Y)$ must be expressed as a polynomial in the $\{G_i\}$, say $m_0(X, Y)=f(G_1,..., G_s)$. This says that $m_0(x, y)-f(g_1,..., g_s)=h(x, y)$ is an identity of mxm matrices. Since the T-ideal of identities of mxm matrices is homogeneous in each variable, without loss of generality f may be replaced by a sum of monomials, all of which have x degree $pN+n$ and y degree N. Moreover, since every monomial in f is a product of invariants of lower degree, none of them are of the form $(*)$ for $p+1 \leqslant q \leqslant n-1$. Proposition 2 now applies to show that $m<p+2=n-t+2$.

3. PROOF OF THE MAIN THEOREM

We now combine the results of Sections 1 and 2.

THEOREM 3. *Let $G=\langle g\rangle$ be a cyclic group of order n acting linearly on $U=k\{X_1,..., X_d\}$, the generic matrix algebra of mxm matrices over the field k, where $d, m \geqslant 2$, and let A be the matrix corresponding to g. Assume that n*

is a unit in k and that A is not scalar. Then U^G *is not finitely generated whenever* $m \geqslant n - [\sqrt{n}] + 1$.

Moreover, if A has a characteristic root α *such that* $\alpha^q = 1$, *some q with* $0 < q < n$, *then* U^G *is not finitely generated whenever* $m \geqslant 2$.

Proof. We assume on the contrary that U^G is finitely generated over k. First, we may assume that k is algebraically closed. For, if not, consider $U_1 = U \otimes_k E$, where E is the algebraic closure of k. Then $U_1 \cong E\{X_1, ..., X_d\}$ and G acts on U_1 by letting it act trivially on E. Since $U_1^G = U^G \otimes E$, U_1^G is finitely generated over E_1 and we may consider U_1 instead of U.

Second, say $G = \langle g \rangle$ and let $A \in \mathrm{Mat}_d(k)$ be the matrix corresponding to g (i.e., $A = (\alpha_{ij})$, where $X_i^g = \sum_j \alpha_{ij} X_j$). We may assume that A is diagonal. For, since $A^n = I$, the minimum polynomial of A divides $x^n - 1$, which has distinct roots since $n^{-1} \in k$. Thus A is diagonalizable, say $B^{-1}AB = \mathrm{diag}(\alpha_1, ..., \alpha_d)$. But now B determines an element l of $\mathrm{Aut}_k(U)$; thus we replace g by $h = l^{-1}gl$, since $U^{\langle h \rangle}$ will also be finitely generated, and h acts by a diagonal matrix. Thus we may assume that $X_i^g = \alpha_i X_i$, all $i = 1, ..., d$.

Now for any i, j, let $U_{ij} = k\{X_i, X_j\}$; there is an induced action of G on U_{ij}, and U_{ij}^G is finitely generated over k since it is a homomorphic image of U^G (by sending $X_l \to 0$, for $l \neq i, j$).

We now consider the characteristic roots of A. Say that A has a root α_i so that $\alpha_i^q = 1$, some $1 < q < n$. Now all the characteristic roots can not have order q, since then $A^q = I$, so $g^q = 1$, which contradicts the fact that g has order n. Thus A must have a characteristic root α_j so that $o(\alpha_j) \neq o(\alpha_i)$. Passing to U_{ij} and applying Theorem 1, we see that U_{ij}^G can not be finitely generated if $m \geqslant 2$, a contradiction.

We may therefore assume that $o(\alpha_i) = n$, all $i = 1, ..., d$. Since G is not scalar, however, two of the roots must be distinct, say $\alpha_1 \neq \alpha_2$. We may write $\alpha_1 = \alpha_2^t$ and $\alpha_2 = \alpha_1^q$, where $1 < t$, $q < n$. Then $\alpha_2 = (\alpha_2^t)^q$, so $tq \equiv 1 \bmod n$. If both $t, q \leqslant \sqrt{n}$, a contradiction. Thus one of them, say $t > \sqrt{n}$. Since t is an integer, $t \geqslant [\sqrt{n}] + 1$. Passing to U_{12}, we may apply Theorem 2 with $\delta = \alpha_2$ to see that $m < n - t + 2$. But $-t \leqslant -[\sqrt{n}] - 1$, and so $m < n - [\sqrt{n}] + 1$, a contradiction.

Remarks. (1) The bound $n - [\sqrt{n}] + 1$ can be improved for some specific choices of n, for the worst possible t for a given n is $t = \min\{1 < s < n \mid (s, n) = 1 \text{ and } s \geqslant s^{-1} \bmod n\}$. Thus for $n = 122$, $t = 35$, and so $n - t + 2 = 89$, the actual bound given by our methods, whereas $n - [\sqrt{n}] + 1 = 112$. Of course, if $n = a(a+1) - 1$ for some a, then $a(a+1) = n + 1$, so $a = [\sqrt{n}]$, $t = a + 1 = [\sqrt{n}] + 1$, and we obtain the bound in the theorem.

On the other hand, no finitely generated nonscalar examples are known other than the example mentioned in the Introduction. Thus we conjecture that when G is not scalar, with $d \geqslant 2$, then U^G is never finitely generated if $m \geqslant 3$.

(2) A major difficulty in extending our theorem to arbitrary finite groups G (acting linearly on U) is a recent result of Guralnick, which asserts that if $|G|$, m, $d \geqslant 2$, then U^G is never a ring of generic matrices [2]. The original proof [1] of the free algebra result proceeds by reducing the problem to cyclic subgroups H of G, using the fact that F^H is again a free algebra. Clearly, this approach will not work for generic matrices.

References

1. W. Dicks and E. Formanek, Poincare series and a problem of S. Montgomery, *Linear and Multilinear Algebra* **12** (1982), 21–30.
2. R. M. Guralnick, Invariants of finite linear groups on relatively free algebras, *Linear Algebra Appl.* **72** (1985), 85–92.
3. N. Jacobson, "*PI* Algebras," Lecture Notes in Math., Vol. 441, Springer–Verlag, New York, 1975.
4. V. K. Kharchenko, Noncommutative invariants of finite groups and Noetherian varieties, *J. Pure Applied Algebra* **31** (1984), 83–90.
5. S. Montgomery, "Trace Functions and Affine Fixed Rings in Noncommutative Rings," Seminaire d'Algebré Paul Dubreil et Marie-Paule Malliavin, Lecture Notes in Math., Vol. 924, pp. 356–374, Springer-Verlag, New York, 1982.
6. S. Montgomery and L. W. Small, Fixed rings of Noetherian rings, *Bull. London Math. Soc.* **13** (1981), 33–38.